Amendments to the Claims:

Please amend claims 1, 29, 56, 59, 61, 85, 89, 111, 112, 115, 126, 129, 131, 155 and 159, please cancel claims 6-10, 31, 58, 64-84, 88, 93-97, 117, 128, 134-154, 158 and 160, and please add new claims 161-174 as follows.

This listing of claims replaces all prior versions, and listings, of claims in the application.

Listing of claims:

1. (Currently Amended) A method for preventing unauthorized use of digital content data comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data; and

storing the modified data at predetermined memory locations;

wherein modifying the data segments further comprises:

encrypting the modified data and storing the encrypted modified data;

encrypting the modified data with an encryption key; and

encrypting the encryption key;

and wherein storing the modified data further comprises:

storing the encryption key with the encrypted modified data at the predetermined memory locations; and

partitioning the encryption key among the encrypted modified data.

2. (Original) The method of claim 1 wherein the digital data comprises data types selected from a group consisting of audio, video, documents, text and software.

3. (Original) The method of claim 1 wherein the data segments are of a variable length

4. (Original) The method of claim 1 wherein the second data comprises a randomly generated data stream.

5. (Original) The method of claim 1 wherein the second data comprises portions of the digital content data.

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Original) The method of claim 1 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

12. (Original) The method of claim 1 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored.

13. (Original) The method of claim 1 further comprising generating a map of locations at which the modified data is stored.

14. (Original) The method of claim 13 further comprising storing the map of locations at the predetermined memory locations.

15. (Original) The method of claim 1 wherein the memory locations reside on a system and further comprising:

scanning the system to determine available memory locations;

selecting target memory locations within the available memory locations at which to store the modified data; and

storing the modified data at the target memory locations.

16. (Original) The method of claim 15 wherein a subset of available memory locations are located within file system locations

17. (Original) The method of claim 15 wherein a subset of available memory locations are located outside file system locations.

18. (Original) The method of claim 15 further comprising generating a map of the target memory locations.

19. (Original) The method of claim 18 further comprising storing the map of target memory locations at the target memory locations.

20. (Original) The method of claim 1 further comprising:

retrieving the modified data from the predetermined memory locations; and

de-interleaving the data segments based on the second data to generate original digital content data.

21. (Original) The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

22. (Original) The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

23. (Original) The method of claim 1 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

24. (Original) The method of claim 23 further comprising, if an authorized access of a file replaced by the modified data is determined, the file is accessed.

25. (Original) The method of claim 1 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data.

26. (Original) The method of claim 1 wherein modifying the data segments with second data comprises tokenizing the data segments with token data.

27. (Original) The method of claim 26 wherein the token data comprises lexical equivalents of assembly language commands.

28. (Original) The method of claim 27 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

29. (Original) A method for preventing unauthorized use of digital content data in a system having memory locations comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data;

scanning the system to determine available memory locations;

selecting target memory locations within the available memory locations at which to store the modified data; and

storing the modified data at the target memory locations,

wherein a subset of the available memory locations are located outside file system

locations.

30. (Original) The method of claim 29 wherein a subset of available memory locations are located within file system locations.

31. (Cancelled)

32. (Original) The method of claim 29 further comprising generating a map of the target memory locations.

33. (Original) The method of claim 32 further comprising storing the map of target memory locations at the target memory locations.

34 (Original) The method of claim 29 wherein the digital data comprises data types selected from a group consisting of audio, video, documents, text and software.

35. (Original) The method of claim 29 wherein the data segments are of a variable length.

36. (Original) The method of claim 29 wherein the second data comprises a randomly generated data stream.

37. (Original) The method of claim 29 wherein the second data comprises portions of the digital content data.

38. (Original) The method of claim 29 further comprising encrypting the modified data and storing the encrypted modified data.

39. (Original) The method of claim 38 further comprising encrypting the modified data with an encryption key.

40. (Original) The method of claim 39 further comprising encrypting the encryption key.

41. (Original) The method of claim 40 further comprising storing the encryption key with the encrypted modified data at the predetermined memory locations.

42. (Original) The method of claim 41 further comprising partitioning the encryption key among the encrypted modified data.

43. (Original) The method of claim 29 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

44. (Original) The method of claim 29 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored.

45. (Original) The method of claim 29 further comprising generating a map of locations at which the modified data is stored.

46. (Original) The method of claim 45 further comprising storing the map of locations at the predetermined memory locations.

47. (Original) The method of claim 29 further comprising:

retrieving the modified data from the predetermined memory locations; and

de-interleaving the data segments based on the second data to generate original digital content data.

48. (Original) The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files

stored on the system, as identified by the table of contents.

49. (Original) The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

50. (Original) The method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

51. (Original) The method of claim 50 further comprising, if an authorized access of a file replaced by the modified data is determined, the file is accessed.

52. (Original) The method of claim 29 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data.

53. (Original) The method of claim 29 wherein modifying the data segments with second data comprises tokenizing the data segments with token data.

54. (Original) The method of claim 53 wherein the token data comprises lexical equivalents of assembly language commands.

55. (Original) The method of claim 54 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data to deter unauthorized access.

56 . (Currently Amended) A method for preventing unauthorized use of digital content data hosted on a system comprising:

modifying the digital content data with saturation data to generate modified data; [[and]]

storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data;

determining whether an unauthorized attempt at accessing the digital content data occurs; and

in the event of unauthorized access, generating saturation traffic on the system to deter the unauthorized activity.

57. (Original) The method of claim 56 further comprising subdividing the digital content data into data segments and modifying the data segments.

58. (Cancelled)

59. (Currently Amended) The method of claim [[58]]56 wherein the saturation traffic comprises system commands that burden system resources.

60. (Original) The method of claim 59 wherein the system commands are generated as a function of activity utilizing the system resources subject to the unauthorized access.

61. (Currently Amended) The method of claim [[58]]56 wherein determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted.

62. (Original) The method of claim 56 further comprising interleaving the digital content data with second data to generate interleaved data.

63. (Original) The method of claim 56 further comprising tokenizing the digital content data with token data.

64. - 84. (Cancelled)

85. (Currently Amended) A method for preventing unauthorized use of digital content data in a system having memory locations comprising:

scanning the system to determine available memory locations based on a file system identifying locations of files on the system;

selecting target memory locations within the available memory locations at which to store the digital content data; and

storing the digital content data at the target memory locations, wherein a subset of the available memory locations are located outside the file system locations.

86. (Original) The method of claim 85 wherein a subset of available memory locations are located within files identified by the file system locations.

87. (Original) The method of claim 85 wherein a subset of available memory locations are located between files identified by the file system locations.

88. (Cancelled)

89. (Currently Amended) A system for preventing unauthorized use of digital content data comprising:

a subdividing unit for subdividing the digital content data into data segments;

a modification unit for modifying the data segments with second data to generate modified data; [[and]]

a storage unit for storing the modified data at predetermined memory locations;

an encryption unit for encrypting the modified data and storing the encrypted

modified data, wherein the encryption unit further encrypts the modified data with an encryption key, wherein the encryption unit further encrypts the encryption key, and wherein the storage unit further stores the encryption key with the encrypted modified data at the predetermined memory locations; and

a partitioning unit for partitioning the encryption key among the encrypted modified data.

90. (Original) The system of claim 89 wherein the data segments are of a variable length

91. (Original) The system of claim 89 wherein the second data comprises a randomly generated data stream.

92. (Original) The system of claim 89 wherein the second data comprises portions of the digital content data.

93. (Cancelled)

94. (Cancelled)

95. (Cancelled)

96. (Cancelled)

97. (Cancelled)

98. (Original) The system of claim 89 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored.

99. (Original) The system of claim 89 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as

combinations of the locations at which the first and second digital content data were originally stored.

100. (Original) The system of claim 89 further comprising a map generator for generating a map of locations at which the modified data is stored.

101. (Original) The system of claim 100 wherein the storage unit further stores the map of locations at the predetermined memory locations.

102. (Original) The system of claim 89 wherein the memory locations reside on the system and further comprising:

a scanner for scanning the system to determine available memory locations;

a selector for selecting target memory locations within the available memory locations at which to store the modified data; and

wherein the storage unit stores the modified data at the target memory locations.

103. (Original) The system of claim 102 wherein a subset of available memory locations are located within file system locations

104. (Original) The system of claim 102 wherein a subset of available memory locations are located outside file system locations.

105. (Original) The system of claim 102 further comprising a map generator for generating a map of the target memory locations.

106. (Original) The system of claim 105 wherein the storage unit stores the map of target memory locations at the target memory locations.

107. (Original) The system of claim 89 further comprising:

means for retrieving the modified data from the predetermined memory locations;

and

means for de-interleaving the data segments based on the second data to generate original digital content data.

108. (Original) The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

109. (Original) The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

110. (Original) The system of claim 89 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

111. (Currently Amended) The system of claim 89 wherein the modification unit modifying~~modifies~~ the data segments comprises interleaving the data segments with the second data to generate interleaved data.

112. (Currently Amended) The system of claim 89 wherein the modification unit modifying~~modifies~~ the data segments with second data comprises tokenizing the data segments with token data.

113. (Original) The system of claim 112 wherein the token data comprises lexical equivalents of assembly language commands.

114. (Original) The system of claim 113 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

115. (Currently Amended) A system for preventing unauthorized use of digital content data in a system having memory locations comprising:

means for subdividing the digital content data into data segments;

means for modifying the data segments with second data to generate modified data;

means for scanning the system to determine available memory locations;

a selector for selecting target memory locations within the available memory locations at which to store the modified data; and

a storage unit for storing the modified data at the target memory locations;

wherein a subset of the available memory locations are located outside file system locations.

116. (Original) The system of claim 115 wherein a subset of available memory locations are located within file system locations.

117. (Cancelled)

118. (Original) The system of claim 115 further comprising a map generator for generating a map of the target memory locations.

119. (Original) The system of claim 118 wherein the storage unit stores the map of target memory locations at the target memory locations.

120. (Original) The system of claim 115 further comprising means for encrypting the modified data and wherein the storage unit stores the encrypted modified data.

121. (Original) The system of claim 120 wherein the means for encrypting further encrypts the modified data with an encryption key.

122. (Original) The system of claim 121 wherein the means for encrypting further encrypts the encryption key.

123. (Original) The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

124. (Original) The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

125. (Original) The system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

126. (Currently Amended) A system for preventing unauthorized use of digital content data hosted on a system comprising:

a modification unit for modifying the digital content data with saturation data to generate modified data; [[and]]

a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data; and.

means for determining whether an unauthorized attempt at accessing the digital content data occurs, and, in the event of unauthorized access, generating saturation traffic on the system to deter the unauthorized activity.

127. (Original) The system of claim 126 further comprising subdividing the digital content data into data segments and modifying the data segments.

128. (Cancelled)

129. (Currently Amended) The system of claim [[128]]126 wherein the saturation traffic comprises system commands that burden system resources.

130. (Original) The system of claim 129 wherein the system commands are generated as a function of activity utilizing the system resources subject to the unauthorized access.

131. (Currently Amended) The system of claim [[128]]126 wherein the means for determining whether an unauthorized attempt at accessing the digital content data occurs monitors activity of the system hosting the digital content data and determines whether the activity is inconsistent with the type of digital content data being hosted.

132. (Original) The system of claim 126 further comprising means for interleaving the digital content data with second data to generate interleaved data.

133. (Original) The system of claim 126 further comprising means for tokenizing the digital content data with token data.

134.-154. (Cancelled)

155. (Currently Amended) A system for preventing unauthorized use of digital content data in a system having memory locations comprising:

a scanner for scanning the system to determine available memory locations based on a file system identifying locations of files on the system;

means for selecting target memory locations within the available memory locations at which to store the digital content data; and

a storage unit for storing the digital content data at the target memory locations, wherein a subset of the available memory locations are located outside the file system locations.

156. (Original) The system of claim 155 wherein a subset of available memory locations are located within files identified by the file system locations.

157. (Original) The system of claim 155 wherein a subset of available memory locations are located between files identified by the file system locations.

158. (Cancelled)

159. (Currently Amended) A system for preventing unauthorized use of digital content data in a system having memory locations wherein the system enables a user to select from a plurality of tool modules, each module providing a service for protecting digital content from unauthorized use such that a user can protect digital content, wherein the tool modules comprise modules that perform functions selected from the group of functions consisting of: interleaving; tokenization; obfuscation; saturation; translocation; shimming and assassination.

160. (Cancelled)

161. (New) A method for preventing unauthorized use of digital content data comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data; and

storing the modified data at predetermined memory locations;

wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents, and wherein, if an authorized access of a file replaced by the modified data is determined, the file is accessed.

162. (New) The method of claim 161 wherein the data segments are of a variable length.

163. (New) The method of claim 161 wherein the second data comprises a randomly generated data stream.

164. (New) The method of claim 161 wherein the second data comprises portions of the digital content data.

165. (New) The method of claim 161 wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

166. (New) The method of claim 161 wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

167. (New) A method for preventing unauthorized use of digital content data comprising:

subdividing the digital content data into data segments;

modifying the data segments with second data to generate modified data; and

storing the modified data at predetermined memory locations;

wherein modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands.

168. (New) The method of claim 167 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

169. (New) The method of claim 167 wherein the data segments are of a variable length.

170. (New) The method of claim 167 wherein the second data further comprises a randomly generated data stream.

171. (New) The method of claim 167 wherein the second data further comprises portions of the digital content data.

172. (New) The method of claim 167 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

173. (New) The method of claim 167 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

174. (New) The method of claim 167 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

175. (New) A system for preventing unauthorized use of digital content data comprising:

a subdividing unit for subdividing the digital content data into data segments;

a modification unit for modifying the data segments with second data to generate modified data; and

a storage unit for storing the modified data at predetermined memory locations;

wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and the token data comprises lexical equivalents of assembly language commands.

176. (New) The system of claim 175 wherein the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access.

177. (New) The system of claim 175 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

178. (New) The system of claim 175 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

179. (New) The system of claim 175 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.

180. (New) A system for preventing unauthorized use of digital content data comprising:

a subdividing unit for subdividing the digital content data into data segments;

a modification unit for modifying the data segments with second data to generate modified data; and

a storage unit for storing the modified data at predetermined memory locations;

wherein the memory locations reside on the system and further comprising:

a scanner for scanning the system to determine available memory locations;

a selector for selecting target memory locations within the available memory locations at which to store the modified data; and

wherein the storage unit stores the modified data at the target memory locations and wherein a subset of available memory locations are located outside file system locations.

181. (New) The system of claim 180 wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents.

182. (New) The system of claim 180 wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents.

183. (New) The system of claim 180 wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents.